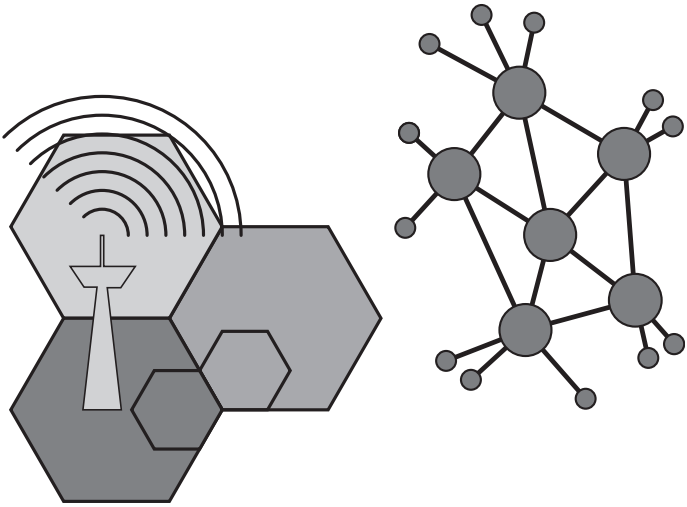
UNIVERSITÄT SIEGEN
Institut für Digitale Kommunikationssysteme

Forschungsberichte

Band 40 Herausgeber: Univ.-Prof. Dr. Christoph Ruland



Jochen Saßmannshausen

Attribute-based Access Control for Smart Grids and Industrial Automation and Control Systems

2020

SHAKER VERLAG

Attribute-based Access Control for Smart Grids and Industrial Automation and Control Systems

DISSERTATION
zur Erlangung des Grades eines Doktors
der Ingenieurwissenschaften

vorgelegt von
M. Sc. Jochen Saßmannshausen
geb. am 05.09.1991 in Siegen

eingereicht bei der Naturwissenschaftlich-Technischen Fakultät
der Universität Siegen
Siegen 2020

1. Gutachter: Prof. Dr. rer. nat. Christoph Ruland
2. Gutachter: Prof. Dr. Hossam Gaber
Vorsitzender: Prof. Dr.-Ing. Roman Obermaisser

Tag der mündlichen Prüfung: 27.05.2020

UNIVERSITÄT SIEGEN

Institut für
Digitale Kommunikationssysteme

Forschungsberichte

Herausgeber: Univ.-Prof. Dr. Christoph Ruland

Band 40

Jochen Saßmannshausen

Attribute-based Access Control for Smart Grids and Industrial Automation and Control Systems

SHAKER VERLAG

Düren 2020

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Siegen, Univ., Diss., 2020

Printed in Germany.

ISBN 978-3-8440-7507-6
ISSN 1614-0508

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren
Phone: 0049/2421/99011-0 • Telefax: 0049/2421/99011-9
Internet: www.shaker.de • e-mail: info@shaker.de

Abstract

Automation and control systems of the industrial sector (Industry 4.0) and the energy supply (Smart Grids) undergo a transformation towards intelligent systems, and previously not connected components are interconnected via local networks and the Internet. Processes are controlled by autonomous computer systems or by operators in remote control centers. The increased number of interconnections between system components softens the principle of a clear separation between traditional information technology (IT) and operational technology (OT) networks. Formerly isolated networks are accessible by an increased number of system components that are not necessarily related with OT processes. Threats to OT systems are both external attackers as well as internal attackers that already have access to a system. Security measures include implementation of communication security protocols as well as access control mechanisms. The goal of access control systems is to restrict access privileges of users/entities (subjects) to a necessary minimum (*Need-to-know principle*). Access privileges of subjects are not static but can change dynamically depending on context and situational factors.

This thesis sets the focus on attribute based access control (ABAC) and its application in Smart Grids and Industrial Automation and Control Systems (IACS), where it is intended to protect process data from unauthorized access. An attribute-based access control framework is developed using a bottom-up security approach that focuses on security and integrity of all systems and information involved in the access control process. The overall system includes system components that evaluate and enforce access control rules as well as systems for distribution of required security information. Management systems allow administrations to edit security properties (attributes) of subjects and protected data objects as well as access rules (policies) that are basis of an authorization process. The developed ABAC framework uses attribute certificates

to represent security properties of subjects and protected data objects. Trusted authorities are able to issue these attribute certificates, which can be verified using a public key infrastructure (PKI). Risk of access depends not only on the accessed data objects themselves, but also on content of commands such as parameters and parameter values that are written to protected data elements. The management systems allow definition of situation-dependent conditions that must be fulfilled for data access. The developed security solution bases on LDAP for storage and distribution of security information and on XACML for definition of access control policies.

The ABAC framework and its associated management systems base on standardized technologies, but the security solution itself is independent of standards and protocols of any application scenarios (e.g. IEC 61850 with security according to IEC 62351-3 and -4). Defined interfaces enable integration of the ABAC framework into concrete application scenarios. The access control system can be integrated into end devices and in form of an application firewall for protection of legacy devices. A proof-of-concept implementation integrates the ABAC framework into an application firewall for the Smart Grid standard IEC 61850. The performance of the developed software is evaluated on multiple platforms with different capabilities.

Zusammenfassung

Im Zuge der Automatisierung von Prozessen im industriellen Bereich (Industrie 4.0) und in der Energieversorgung (Smart Grids) findet eine zunehmende Vernetzung vormals nicht vernetzter Komponenten durch lokale Netzwerke und das Internet statt. Prozesse können autonom durch Computersysteme und aus der Ferne durch Leitstellen gesteuert werden. Die zunehmende Vernetzung von Systemkomponenten weicht die Grenzen zwischen Netzwerken der klassischen Informationsverarbeitung und Netzwerken zum Zweck der Prozesssteuerung auf. Vormals voneinander isolierte Netzwerke sind nun von einer Vielzahl von Systemkomponenten zugreifbar. Zu den Bedrohungen der vernetzten Systeme gehören sowohl externe Angreifer als auch interne Angreifer, die bereits Zugang zu einem System haben. Schutzmaßnahmen beinhalten den Einsatz von Kommunikationssicherheitsprotokollen und Zugriffskontrolle, wobei die Zugriffsrechte von Benutzern/Geräten/Prozessen (Subjekten) auf das absolute notwendige Minimum beschränkt werden müssen (*Need-to-know-Prinzip*). Die Zugriffsrechte sind jedoch nicht statisch, sondern können sich situationsbedingt ändern.

Diese Arbeit befasst sich mit der attribut-basierten Zugriffskontrolle (ABAC) zum Schutz von Daten in intelligenten Energienetzen (Smart Grids) und in industriellen Steuersystemen. Im Rahmen dieser Arbeit wird ein Framework für den Einsatz von attribut-basierter Zugriffskontrolle entwickelt, wobei die Sicherheit und Integrität aller an der Zugriffskontrolle beteiligten Systeme und Informationen gewährleistet wird. Das entwickelte Gesamtsystem umfasst die Systemkomponenten, welche Zugriffsregeln auswerten und anwenden, Systeme zur Übermittlung der dazu benötigten Informationen und zuletzt auch Managementsysteme, die es autorisierten Administratoren erlauben, Sicherheitseinstellungen vorzunehmen. Die Managementsysteme verwalten Sicherheitsattribute von Subjekten und geschützten Datenobjekten und darüber hinaus auch die Zugriffsregeln (Policies) selbst. Sicherheitseigenschaften von Subjekten und Ob-

jekten werden durch Attributzertifikate repräsentiert, die von autorisierten *Attribute Authorities* erstellt werden und mit den Mechanismen einer Public-Key-Infrastruktur (PKI) verifiziert werden können. Management-Systeme erlauben die Definition von situationsabhängigen Bedingungen, die für den Zugriff auf Datenobjekte erfüllt sein müssen, da das Risiko von Zugriffen nicht nur von den Datenobjekten selbst abhängt, sondern auch von Parametern und Parameterwerten, die geschrieben werden sollen. Die entwickelte Sicherheitslösung realisiert das Management und die Verteilung von Sicherheitsinformationen unter Verwendung eines LDAP-Servers und setzt den XACML-Standard für die Definition und die Auswertung von Policies ein.

Die Entwicklung des ABAC-Frameworks und der zugehörigen Managementsysteme basiert auf standardisierten Technologien, die Sicherheitslösung selbst ist jedoch unabhängig von Standards und Protokollen möglicher Anwendungsszenarien (z.B. IEC 61850 mit Security nach IEC 62351-3 und -4). Zur Integration in konkrete Anwendungsszenarien werden definierte Schnittstellen bereitgestellt. Das Zugriffskontrollsystem kann sowohl in Endgeräten als auch in Form einer Firewall für Legacy-Geräte zum Einsatz kommen. Die Anwendung des entwickelten Sicherheitssystems wird am Beispiel einer Application Firewall für den Smart-Grid-Standard IEC 61850 demonstriert. Die Performance der entwickelten Software wird auf verschiedenen Plattformen mit unterschiedlicher Leistungsfähigkeit analysiert.

Acknowledgments

This thesis was created during my employment at the Chair for Data Communications Systems at the University of Siegen.

First and foremost, I would like to express my sincere gratitude to my advisor Prof. Dr. rer. nat. Christoph Ruland for his continuous support and many valuable discussions during my research and my regular tasks at the institute. The creation of this work would not have been possible without his dedication. I would also like to thank him for the opportunity to gather valuable experience in both national and international standardization.

My sincere thanks go to Prof. Dr. Hossam Gaber who agreed to be the second reviewer for my thesis. Furthermore, I would like to thank Prof. Dr.-Ing Roman Obermaisser who chaired the examination commission as well as Prof. Dr. rer. net. Roland Wismüller and Prof. Dr. rer. nat. habil. Frank Gronwald who agreed to be members of the examination commission.

I would like to thank my current and former colleagues Matthias Schneider, Martin Kramer, Natasa Zivic, Robin Fay, Thomas Koller, Tao Wu, Romeo Ayemele Djeujo, Wilfried Kahle and Obaid Ur-Rehman. My thanks also go to my colleagues from the Chair for Embedded Systems for many valuable discussions and their continuous support.

Finally, I would like to thank my family and friends and especially Bianca Schneider for their continuous support throughout my life and particularly during the time I worked on this thesis.

Contents